No. 13-1181

IN THE
Supreme Court of the United States

GOOGLE INC.,

Petitioner,

v.

JOFFE ET AL.,

Respondents.

On Petition for a Writ of Certiorari
to the United States Court of Appeals
for the Ninth Circuit

BRIEF FOR INFORMATION TECHNOLOGY & INNOVATION FOUNDATION AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

MICHAEL S. KWUN
Counsel of Record
ASHOK RAMANI
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, CA 94111
mkwun@kvn.com
(415) 391-5400

April 30, 2014

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Statutes

Legislative Material

Other Authorities

INTEREST OF AMICUS CURIAE[1]

The Information Technology and Innovation Foundation ("ITIF") files this brief to inform the Court of the serious consequences that will result if the ruling below is not reviewed. That impact will extend to all aspects of the economy that rely on wireless technology infrastructure, including but not limited to healthcare, financial institutions, retailers and residential computer users.

ITIF, a 501(c)(3) nonprofit organization founded in 2006, is a non-partisan research and educational institute—a think tank. Its mission is to formulate and promote public policies to advance technological innovation and productivity internationally, in Washington, and in the states. Recognizing the vital role of technology in ensuring prosperity, ITIF focuses on innovation, productivity and digital economy issues. ITIF believes that technological innovation, particularly in information technology, is at the heart of America's growing economic prosperity. ITIF further believes that crafting effective policies that boost innovation and encourage the widespread "digitization" of the economy is

[1] The parties have consented to the filing of this brief. Counsel of record for all parties received notice at least 10 days prior to the due date of the intention of ITIF to file this brief. No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than ITIF or its counsel made a monetary contribution to its preparation or submission.

critical to ensuring robust economic growth and an improved standard of living. ITIF's mission is to help policy makers at the federal and state levels to better understand the nature of the new innovation economy and the types of public policies needed to drive innovation, productivity and broad-based prosperity for all Americans.

ITIF publishes policy reports, holds forums and policy debates, advises elected officials and their staff, and is an active resource for the media. Among other things, ITIF also analyzes existing policy issues through the lens of advancing innovation and productivity, and opposes policies that hinder digital transformation and innovation.

Consistent with its mission and its other work, ITIF files this brief to urge the Court to grant the petition, to reverse the court of appeals, and to interpret "radio communication" to have its plain meaning, which is a communication sent using radio frequency signals.

SUMMARY OF ARGUMENT

ITIF supports the petition, which raises an important issue of federal law that has not been, but should be, addressed by the Court. The court of appeals erred, and absent review of its decision, information technology ("IT") professionals across the country will be left in legal limbo, uncertain whether standard practices they use every day to secure and optimize wireless infrastructure violate the Wiretap Act.

Under the Wiretap Act, one who intentionally intercepts an electronic communication can be subject to criminal and civil liability. If, however, the intercepted electronic communication is a *radio* communication, then the Wiretap Act does not prohibit the interception unless one of several conditions is met, such as that the signal is scrambled or encrypted.

The court of appeals, however, held that a "radio communication" is limited to a "predominantly auditory broadcast," thus excluding a variety of modern radio communications, including those on Wi-Fi networks. The court of appeals relied in large part on a specific set of exemptions from liability in the Wiretap Act that were developed to shield old-world, traditional radio activities, such as listening to AM/FM radio, monitoring public safety radio frequencies, or listening to ham or CB radio.

But Congress drafted exemptions not only for those traditional radio services, but also an exemption applicable to modern *electronic* communications—including electronic *radio* communications—that are readily accessible to the general public. The court of appeals' narrow interpretation of "radio communication" cannot be squared with Congress's intent to modernize the Wiretap Act.

Based on the statutory definition of "readily accessible to the general public" that is applicable to radio communications, the Court should grant the petition and hold that an *unsecured* Wi-Fi communication is readily accessible to the general

public. This conclusion would harmonize the Act's treatment of old-world, traditional radio communications with its treatment of modern electronic communications, and particularly modern electronic *radio* communications.

What "radio communication" means is an important question of federal law, because the narrow definition adopted by the court of appeals calls into question the legality of standard techniques used by IT professionals across the country every day to secure and optimize wireless networks. The lack of clarity that results from the court of appeals' decision makes it *harder* for IT professionals to secure wireless networks, threatening the security of our nation's wireless infrastructure.

ITIF urges the Court to confirm that standard IT practices used to secure wireless networks do not violate the Wiretap Act. ITIF urges the Court to grant the petition and reverse the judgment of the court of appeals.

ARGUMENT

I. *The court of appeals erred.*

The 1986 amendments to the Wiretap Act recognized that the Act had "not kept pace with the development of communications and computer technology."[2] Providing a generalized, technology

[2] S. Rep. No. 99-541, at 2 (1986).

neutral definition of when communications by radio are readily accessible the general public—rather than relying on specific exemptions based on old-world technologies, as the court of appeals did—is consistent with Congress's intent to modernize the Wiretap Act.

Under the Wiretap Act, one who intentionally intercepts an electronic communication can be subject to criminal and civil liability.[3] But there are many exceptions to this general rule. The exception relevant here is that it is not unlawful "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is *readily accessible to the general public*."[4]

The Act provides that a "*radio* communication" is readily accessible to the general public unless one of several conditions is met.[5] Directly relevant here, a radio communication that is "scrambled or encrypted" is not readily accessible to the general public.[6]

The court of appeals correctly observed that "[a]lthough § 2511(2)(g)(i) does not use the words 'radio communication,' the statute nevertheless directs us to apply the § 2510(16) definition to the

---

[3] 18 U.S.C. § 2511(1), (4) & (5).

[4] *Id.* § 2511(2)(g)(i) (emphasis added).

[5] *Id.* § 2510(16) (emphasis added).

[6] *Id.* § 2510(16)(A).

§ 2511(2)(g)(i) exemption." App. 8a–9a. [7] Combining sections 2511(2)(g)(i) and 2510(16) yields an exemption from liability for interception of an *electronic* communication that is a *radio* communication, if none of the exceptions in section 2510(16) (such as scrambling or encryption) apply.

The Wiretap Act does not include an express definition of "radio communication," but for the reasons given in the petition, "radio communication" must mean "communication by radio." Pet. 10–13. That is the plain meaning of the term, and also the only meaning that is consistent with how the term is used in the Wiretap Act. Pet. 13–18. ITIF submits that Petitioner's arguments are compelling, and merit granting the petition.

In addition to the reasons offered by Petitioner, for the reasons given below, the court of appeals' interpretation—limiting a radio communication to "a predominantly auditory broadcast," App. 14a–15a—would render the express definition of "readily accessible to the general public" for a "radio communication" all but meaningless in the context of section 2511(2)(g)(i). But if instead, as urged by

[7] Section 2511(2)(g)(i) is an exemption for interception of certain electronic communications. Some electronic communications are radio communications. 18 U.S.C. § 2510(12) (subject to certain exceptions, an electronic communication includes signals "transmitted in whole or in part by a . . . radio . . . system"). And the definitions in section 2510 apply to "this chapter," of which section 2511(2)(g)(i) is a part.

Petitioner, "radio communication" means a communication by radio, this outcome is avoided.

The court of appeals held that a "radio communication" must be a "predominantly auditory broadcast," concluding that the uses of the term in the Wiretap Act "evoke traditional radio technologies." App. 17a. In so concluding, the court of appeals leaned heavily on the Act's exemptions in section 2511(2)(g)(ii) for "intercepting" traditional radio broadcasts. *Id.*

The section 2511(2)(g)(ii) exemptions for traditional radio services keep the Wiretap Act from criminalizing turning on an AM/FM radio, using a radio scanner to monitor public safety services, listening in on ham radio or CB chatter, or air traffic control frequencies and the like.[8] These exemptions apply to radio communications that are overwhelmingly likely to include the human voice and be transferred, at least in part, by wire.

But the exemption in section 2511(2)(g)(i) is limited to *electronic* communications, *which excludes communications that include the human voice and are transferred in part by wire.* By statutory definition, an electronic communication cannot be a wire communication,[9] and a communication is a wire

[8] *Id.* § 2511(2)(g)(ii)(I)-(IV).

[9] *Id.* § 2510(12)(A).

communication if it includes the human voice and is transferred, at least in part, by wire.[10]

Section 2511(2)(g)(i) therefore for the most part *excludes* interception of traditional radio broadcasts such as listening to AM/FM broadcasts or using a police scanner, because those communications typically occur at least in part by wire and include human voices.[11] Thus, incongruously, the court of appeals (a) recognized that the definition of when a radio communication is readily accessible to the general public applies to electronic communications; while (b) simultaneously defining "radio communication" so narrowly that the definition has no significant applicability to electronic communications.

If the court of appeals' interpretation is correct, the only radio communications for which interception might be exempted by section 2511(2)(g)(i) are "predominantly auditory broadcasts" that do not include the human voice, or that are accomplished without use, even in part, of wire, cables or the like. But interception of voiceless radio broadcasts to the public is exempted by section 2511(2)(g)(ii)(I). And interception of Morse code or other non-voice

---

[10] *Id.* § 2510(1) ("wire communication" includes an "aural transfer" that occurs "in whole or in part" through use of a wire); *id.* § 2510(18) ("aural transfer" means the transfer contains the human voice).

[11] In contrast, the section 2511(2)(g)(ii) exemptions apply to radio communications generally, without any requirement that they also are electronic communications.

communications by amateur radio enthusiasts is already exempted by section 2511(2)(g)(ii)(III). Under the court of appeals' interpretation, it is unclear what radio communications Congress intended to exempt under section 2511(2)(g)(i).

But if Congress had intended that exemptions from liability for interception of radio communications be fully addressed by section 2511(2)(g)(ii), there would have been no need to provide a special definition of "readily accessible to the general public" in section 2510(16). Aside from its definition in section 2510(16), the phrase "readily accessible to the general public" is used only twice in the Wiretap Act, in section 2511(2)(g)(i) and in section 2511(2)(g)(ii)(II). Thus, if section 2511(2)(g)(i) does not exempt interception of any radio communications beyond those that are exempted by section 2511(2)(g)(ii), Congress could have taken the more direct approach of including the substance of section 2510(16) in section 2511(2)(g)(ii)(II).

But that was *not* Congress's intent. Congress intended that sections 2510(16) and 2511(2)(g)(i) act in tandem:

> Radio communications "readily accessible to the general public" are defined in proposed subsection 2510(16). Radio communications are considered readily accessible to the general public unless they fit into one of five specified categories.

> As described below, subsection 101(b) of the Electronic Communications Privacy Act [amending 18 U.S.C. § 2511] provides an exception to the general prohibitions on interception for electronic communications which are configured to be readily accessible to the general public. Thus, the radio communications specified in proposed subsection 2510(16) are afforded privacy protections under this legislation unless another exception applies.[12]

Plainly, Congress intended that section 2511(2)(g)(i) exempt interception of some radio communications that are not exempted by section 2511(2)(g)(ii).

The court of appeals' interpretation of "radio communication" therefore cannot be correct. If the Court instead holds that a radio communication is a communication by radio, then section 2511(2)(g)(i) has a non-duplicative scope for radio communications. Under this interpretation, there would be a straightforward rule that interception of unsecured electronic communications by radio should not be criminalized, unless one of the other conditions in section 2510(16) is met.[13]

---

[12] S. Rep. No. 99-541, at 14–15.

[13] For example, even if not scrambled or encrypted, interception of an electronic communication by radio would not be exempted from liability if essential parameters for demodulating the communication were withheld from the public in order to protect privacy. 18 U.S.C. § 2510(16)(B).

II. *Wi-Fi communications are readily accessible to the general public just as public safety radio communications are.*

Most of the general public cannot readily build a radio to listen to unscrambled, unencrypted radio communications on public safety systems. Congress nonetheless had no hesitation concluding that such radio communications are "readily accessible to the general public."[14] And Congress was correct, because the general public *can* readily access such communications using commonly available, off-the-shelf radio scanners. Because those communications are readily accessible to the general public, intercepting them does not violate the Wiretap Act.[15]

Similarly, members of the general public can (and do) readily access Wi-Fi communications using commonly available, off-the-shelf hardware and software—personal computers with Wi-Fi cards. And if a member of the general public wants to inspect Wi-Fi packets other than those addressed to or from the user's computer—that is, to "intercept" those communications[16]—off-the-shelf software suitable for inspecting Wi-Fi packets broadcast *without encryption,* such as the "Wireshark" network protocol

---

[14] *See* 18 U.S.C. § 2510(16).

[15] *Id.* § 2511(2)(g)(ii)(II).

[16] Standard practices in the IT industry regularly require such interception. *See* Part III, *infra.*

analyzer,[17] is also readily accessible to the general public—indeed, it is available for free. Wireshark is "the world's foremost network protocol analyzer," "lets you see what's happening on your network at a microscopic level," and "is the de facto (and often de jure) standard across many industries and educational institutions."[18] The software includes a setting that allows the user to capture all packets on a network segment instead of limiting captured packets to those being sent to and from the user's computer.[19] Wireshark is compatible with standard hardware running Microsoft Windows, Apple Mac OS X, and many other operating systems.[20]

---

[17] Wireshark Foundation, *Wireshark • Go Deep,* http://www.wireshark.org. The list of developers who have contributed code to Wireshark includes email addresses from, among other companies, Alcatel, Cisco, and NetApp. Wireshark Foundation, *Wireshark • About,* http://www.wireshark.org/about.html (hereinafter, "*Wireshark About Page*"). The software has been named one of the most important open-source applications of all time by *eWeek,* and has also been highly praised by *PC Magazine. See id.*

[18] *Wireshark About Page.*

[19] *See* Wireshark Foundation, *4.6. The "Edit Interface Settings" dialog box,* http://www.wireshark.org/docs/wsug_html_chunked/ChCapEditInterfaceSettingsSection.html ("Capture packets in promiscuous mode" setting). In some circumstances, the user could also need to use an alternate network driver, but in many instances the standard network driver that is already installed on the computer will suffice.

[20] *Wireshark About Page.*

And there is nothing nefarious about this "packet sniffing." Instead, this is precisely what is intended by the Wi-Fi standards. By design, "[i]f the data confidentiality service is not invoked" for a Wi-Fi communication—if the Wi-Fi communication is not encrypted—"all frames are sent unprotected."[21] As the applicable standards state, due to the lack of security on an unencrypted Wi-Fi network, "the connection of a single wireless link (without data confidentiality) to an existing wired LAN may seriously degrade the security level of the wired LAN."[22] In short, unencrypted Wi-Fi communications are not intended to be secure from eavesdropping.

III. *The court of appeals' decision raises an important question of federal law, and calls into question techniques used every day by information technology professionals at companies around the country.*

If, as the court of appeals held, a Wi-Fi communication is *not* a "radio communication," IT professionals are left uncertain whether interception of an unencrypted Wi-Fi communication is lawful. This is an important question of federal law because

---

[21] IEEE Standards Association, *IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* 75 (2012).

[22] *Id.*

IT professionals routinely engage in packet sniffing and subsequent packet analysis to do their jobs.

In particular, IT security professionals use packet sniffing and analysis to comply with various security requirements in, for example, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Sarbanes-Oxley Act. IT security professionals also use packet sniffing and analysis to ensure compliance with, for example, data security standards in the payment card industry such as Visa's Cardholder Information Security Program, and with standards required by the Department of Defense.

Packet sniffing and analysis are valuable, standard tools for IT professionals for a host of reasons:

Detecting unauthorized wireless network access points: IT security professionals can use packet sniffing and analysis to detect unauthorized wireless network access points that could allow attackers onto a corporate network or allow employees to circumvent network security controls. To mitigate this risk, IT security professionals will actively scan for unauthorized access points. Actively scanning for unauthorized access points involves monitoring all wireless traffic to create a list of all access points in use.

Stopping "evil twin" or "WiFishing" attacks: IT security professionals also perform packet sniffing and analysis to detect rogue wireless network access

points ("evil twin" or "WiFishing" attacks). A rogue access point is one that broadcasts the Service Set Identifier ("SSID") of a legitimate access point so that users will inadvertently connect to the rogue network. To mitigate this risk, IT security professionals monitor wireless traffic to detect beacons from unauthorized access points.

Locating unauthorized Wi-Fi devices: IT security professionals can also use packet sniffing and analysis to detect unauthorized Wi-Fi devices. Some organizations prohibit employees from bringing unauthorized wireless devices to their facility. To detect a violation of this policy, organizations might monitor wireless traffic to track the addresses of Wi-Fi devices in operation.

Protecting against network intrusions: Capturing wireless traffic also allows IT security professionals to protect against attacks by detecting active scanning, a probing technique used by intruders to identify wireless networks. Similarly, IT security professionals can capture wireless traffic to analyze wireless packets for malicious or anomalous activities that indicate a potential threat. For example, wireless packet payload data can be analyzed to detect malware, such as computer viruses, or other attack signatures, such as denial of service attacks.

Optimizing network performance: Standard network management practices can also involve monitoring wireless traffic. For example, many Wi-Fi networks operate in the 2.4 GHz spectrum. There

are limited channels available in that spectrum for communicating on a Wi-Fi network. To optimize performance, a home user or company might monitor wireless traffic to determine the optimal channel to use. Because the use of channels can change over time, such analysis might need to be repeated regularly to optimize network performance.

In all of the above cases, an IT professional might capture unencrypted Wi-Fi communications. In dense, urban settings, corporate Wi-Fi networks and home Wi-Fi networks can easily overlap. As a result, IT professionals performing their jobs might well capture packets not only from the corporate network, but also from other networks as well. In fact, without inspecting payload data, in many cases they will not be able to distinguish between activity on an overlapping non-corporate network, which presents no security concerns, and insecure or malicious traffic on the corporate network.

Congress created a bright-line definition of when a radio communication is readily accessible to the general public. That definition allows IT professionals to go about their daily work without fearing prosecution for violating the Wiretap Act. The court of appeals' erroneous, narrow interpretation of "radio communication" subverts Congress's intent. Perversely, the court of appeals' decision threatens to make our nation's computing infrastructure *less* secure, by calling into question practices used by IT security professionals every day to secure wireless networks. As a result, the court of appeals' decision, if not reviewed, will make it harder for IT security

professionals to do their jobs, rendering wireless networks more susceptible to intrusion. This cannot be what Congress intended.

CONCLUSION

Amicus curiae ITIF urges the Court to grant the petition and reverse the judgment of the court of appeals.

Respectfully submitted,

MICHAEL S. KWUN
Counsel of Record
ASHOK RAMANI
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, CA 94111
mkwun@kvn.com
(415) 391-5400

April 30, 2014